Dateneigentum und Datenzugang – Schutz von Geschäftsgeheimnissen als Alternative?

Picht, Peter Georg

Abstract: Die Rechtsregeln zum Geschäftsgeheimnisschutz sind fest etablierter Bestandteil des Schweizer Rechts; Geschäftsgeheimnis-Transaktionen (z.B. Lizenzierung) haben erhebliche ökonomische Bedeutung. Aber eignet sich der Geschäftsgeheimnisschutz auch als zentraler Ordnungsrahmen für die datenbasierte Wirtschaft der Zukunft? Der Beitrag skizziert den gegenwärtigen Rechtsrahmen, misst seine Leistungsfähigkeit am Fallbeispiel der «connected mobility», leitet aus diesem «Praxistest» Problemstellungen ab, leuchtet das Problemlösungspotential der aktuellen Rechtssetzung aus und schliesst mit zwei denkbaren Szenarien für das weitere Vorgehen.

Jusletter IT

Dateneigentum und Datenzugang

Schutz von Geschäftsgeheimnissen als Alternative?

Autor: Peter Georg Picht
Kategorie: Beiträge
Region: Schweiz
Rechtsgebiete: Datenschutz
Zitiervorschlag: Peter Georg Picht, Dateneigentum und Datenzugang, in: Jusletter IT Flash 11. Dezember 2017

Die Rechtsregeln zum Geschäftsgeheimnisschutz sind fest etablierter Bestandteil des Schweizer Rechts; Geschäftsgeheimnis-Transaktionen (z.B. Lizenzierung) haben erhebliche ökonomische Bedeutung. Aber eignet sich der Geschäftsgeheimnisschutz auch als zentraler Ordnungsrahmen für die datenbasierte Wirtschaft der Zukunft? Der Beitrag skizziert den gegenwärtigen Rechtsrahmen, misst seine Leistungsfähigkeit am Fallbeispiel der «connected mobility», leitet aus diesem «Praxistest» Problemstellungen ab, leuchtet das Problemlösungspotential der aktuellen Rechtssetzung aus und schliesst mit zwei denkbaren Szenarien für das weitere Vorgehen.

Inhaltsverzeichnis

I. Bestehender Rechtsrahmen

[Rz 1] Die Normbasis für den Schutz von Geschäftsgeheimnissen im heutigen schweizerischen Recht verteilt sich auf eine ganze Reihe von Vorschriften. Auf völkerrechtsvertraglicher Ebene besonders wichtig[1] ist Art. 39 der Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS), der die Vertragsstaaten des Abkommens auf den (lauterkeitsrechtlichen) Schutz von Informationen verpflichtet, sofern diese einen kommerziellen Wert aufweisen, zum Gegenstand von sachgerechten Geheimhaltungsmassnahmen gemacht wurden und nicht allgemein verfügbar sind. Art. 4 lit. c und Art. 6 des Bundesgesetzes gegen den unlauteren Wettbewerb (UWG) erklären es als unlauter, unrechtmässig erlangte Fabrikations- und Geschäftsgeheimnisse mitzuteilen oder zu verwerten. Art. 5 UWG verbietet insbesondere das unbefugte Verwerten fremder Arbeitsergebnisse. Art. 321a Abs. 4 des Obligationenrechts (OR) etabliert eine Pflicht des Arbeitnehmers zur Verschwiegenheit und Nichtverwertung in Bezug auf Geschäftsgeheimnisse des Arbeitgebers. Art. 162 des Strafgesetzbuches (StGB) stellt die Verletzung einer gesetzlichen oder vertraglichen Pflicht zur Bewahrung eines Geschäftsgeheimnisses auf Antrag unter Strafe.

[Rz 2] Aus der Zusammenschau dieser Normen wird deutlich, dass das nationale schweizerische Recht zum Schutz von Wirtschaftsgeheimnissen einen etwas fragmentierten Charakter hat und dass seine Umgrenzung des schutzwürdigen Bereichs von dem eher restriktiven Konzept des Unternehmensgeheimnisses geprägt ist, nicht von einem weiter verstandenen Know-how-Konzept. Grundsätzlich bedarf es für den Schutz also der vier Kernvoraussetzungen (1) unbekannte Tatsache, (2) objektiv schutzwürdiges Geheimhaltungsinteresse, (3) subjektiver Geheimhaltungswille und (4) Zugehörigkeit zum unternehmerischen Bereich.[2] Ein weit verstandener Know-how-Begriff kann hingegen insbesondere auch nicht-geheime Inhalte erfassen, wird allerdings andererseits eher auf technisch direkt anwendbares Wissen bezogen.[3]

[Rz 3] Zudem und vor allem werden Informationen nicht als solche gegenüber allen Teilnehmern des Rechtsverkehrs geschützt. Vielmehr ist der Schutz durch die Abwehr bestimmter Verhaltensweisen (Verhaltensunrecht) von Seiten bestimmter Personengruppen gekennzeichnet.[4] Und stets muss sich die Information, um schutzfähig zu sein, im Aggregatzustand der Geheimhaltung befunden haben. Wer also – und dies wird für den weiteren Gang der hiesigen Überlegungen wichtig sein – die Informationen teilt, verliert den Schutz für sie, sofern er nicht (insbesondere durch Geheimhaltungsvereinbarung) ihren – mehr oder weniger fiktionalen – Geheimnischarakter aufrechtzuerhalten vermag. Unabhängig davon, ob man den Normen zum Schutz von Geschäftsgeheimnissen bereits heute den Gehalt der positiven Zuweisung einer Rechtsposition an den Geheimnisherren entnehmen will oder die stärkere Ausprägung einer Zuweisungsfunktion für die Zukunft fordert[5] – jedenfalls sind Geschäftsgeheimnisse derzeit nicht Gegenstand eines Immaterialgüterrechts, das nach Art von Patenten oder Urheberrechten exklusive Nutzung und weitreichende Verbotsrechte trotz Offenlegung des Schutzgegenstandes sichern würde.[6] All dies macht Geschäftsgeheimnisse in gewisser Weise zu einem fragilen Geschäftsgegenstand: Die Zuweisung einer Inhaberschaft, ja der Rechtsposition selbst, welche Transaktionen in Bezug auf das Geschäftsgeheimnis überhaupt erst ermöglicht, hängt weniger von einer rechtlichen Bewertung der ökonomischen Schutzwürdigkeit ab, als vielmehr von einer faktischen, geheim haltenden Kontrolle, die verhältnismässig leicht verloren gehen kann. Nichtsdestotrotz sind Geschäftsgeheimnisse in heutigen Volkswirtschaften von sehr hohem, ja in der «Wissensgesellschaft» von zunehmendem Wert und sie bilden den Gegenstand intensiver Transaktionstätigkeit. Hierin erweist sich zugleich die gestalterische und ordnende Kraft des Marktes auch im Umgang mit fragmentarisch geregelten Konstellationen.

II. Geheimnisschutz als Ordnungsrahmen für die Datenwirtschaft? Modellszenario «connected mobility»

[Rz 4] Auf den ersten Blick macht dieser Befund Mut, wenn es um die Frage geht, ob die Regeln zum Schutz von Geschäftsgeheimnissen einen sachgerechten Ordnungsrahmen für die sich entwickelnde Datenwirtschaft setzen können. Weshalb sollte der Erfindungsreichtum der Marktteilnehmer, gestützt auf das flexible Instrument des schuldrechtlichen, nur relativ zwischen den Parteien wirkenden Vertrages, nicht auch tragfähige Lösungen für digitale Know-how-Geschäftsgegenstände schaffen können? Blickt man indes auf konkrete Anwendungsfälle aus den komplexeren Bereichen der Datenwirtschaft, wie etwa die «connected mobility» (besonders prominent: autonomes Fahren), sinkt der Mut doch etwas. Denn es wird klar, dass der Geschäftsgeheimnisschutz in seiner gegenwärtigen, hergebrachten Gestalt keine fertigen Antworten auf eine ganze Reihe von Fragen parat hält, die solche Konstellationen aufwerfen.

1. Mobilitätsdaten – Geschäftsgeheimnisse?

[Rz 5] Weder das Praxisbeispiel der connected mobility noch die sich aus ihm ergebenden Überlegungen zur Ausgestaltung des Geheimnisschutzes können im vorliegenden Rahmen voll entfaltet werden.[7] Herausgegriffen sei aber, als ein erster Gesichtspunkt, die vielfältige und nicht durchweg klassischen Mustern des Geheimnisschutzes entsprechende Struktur der generierten Daten. Bewegungsdaten privater Verkehrsteilnehmer etwa sind weder deren geschäftlichem Bereich zuzuordnen noch wahrhaft geheim, da sie unverzüglich an verschiedene, Daten sammelnde und Daten speichernde Akteure übermittelt werden – und zudem sehr häufig an

alle in optischer oder sonst durch Sinne vermittelter Reichweite befindlichen übrigen Verkehrsteilnehmer. Als Geschäftsgeheimnisse im klassischen Sinne drängen sie sich mithin nicht auf. Anders kann die Bewertung schon ausfallen, wenn eine Vielzahl von Nutzerdaten aggregiert und mittels ihrer vergleichenden Auswertung ein Befund über bestimmte Umweltgegebenheiten oder Verhaltensmuster gewonnen wird. Das Geheimnisschutzrecht müsste sich hier also entscheiden, ob und auf welcher Ebene Schutz für «Folgedaten» bzw. Datenprodukte selbst dann bestehen soll, wenn die Ausgangsdaten nicht geheimnisschutzfähig sind.

2. Zuordnung von Nutzungsbefugnis und ökonomischem Potential

[Rz 6] Sind die schutzfähigen Datengegenstände abgegrenzt, gilt es, über den Schutzbegünstigten zu entscheiden. Wer darf also insbesondere über die ökonomische Verwertung der Daten bestimmen? Um mit dem Bild des Verkehrsprobleme verursachenden Schlaglochs auf der Strasse zu sprechen: Ist die wirtschaftliche Zuordnung zum Fahrer eines über das Schlagloch rumpelnden Wagens sachgerecht, weil dieser das Datum mit seinem Verhalten generiert; zum Halter, weil auch das Fahrzeug für die Datengenerierung erforderlich ist; zum Hersteller des Bewegungssensors, weil ohne diesen das Datum nicht aufgezeichnet werden könnte; zum Hersteller des Autos, weil dieser das in seiner Gesamtheit Daten generierende System bereitstellt; zum Betreiber der Strasse, weil auch diese Infrastruktur in ihrer Fehlerhaftigkeit an der Generierung des Datums einen unverzichtbaren Anteil hat; zum Inhaber bzw. Betreiber des Software- und Kommunikationssystems, das aus der Vielzahl einzelner Begegnungen von Fahrzeugen mit dem Schlagloch den Befund einer Verkehrsstörung erhebt und hieraus möglicherweise zugleich die Empfehlung eines Umweges ableitet, weil erst auf dieser Ebene das Nutzenpotential des einzelnen Datums voll realisiert wird?

[Rz 7] Die hergebrachte Antwort des Geheimnisschutzes wäre wohl die Begünstigung desjenigen Akteurs, der als erster unternehmerisch mit den Informationen agiert und faktisch deren Geheimhaltung bewerkstelligt. Und in der Tat sind es gegenwärtig häufig die faktischen Inhaber der «Schnittstellenkompetenz», welche auch die an der Schnittstelle gesammelten Daten kontrollieren.[8] Insbesondere im Verhältnis zu den ihre Daten – *nolens volens* – preisgebenden Privatakteuren sind an einer pauschalen Verwendung dieses Zuordnungsprinzips indes Zweifel gerechtfertigt. Soll sich aber die Zuordnung der ökonomischen Verwertungsbefugnis beispielsweise stärker daran orientieren, wer einerseits relevante Investitionsbeiträge zum Entstehen des verwertbaren Informationsprodukts geleistet hat, und dass andererseits eine – ggf. entgeltliche – Zugänglichkeit der Daten(produkte) für Miterzeuger und Dritte erhalten bleibt,[9] muss das Geheimnisschutzrecht in diesem Gesichtspunkt kritisch überdacht werden.

3. Interaktion mit anderen Rechtsgebieten

[Rz 8] Beim Zusammentreffen von Geheimnisschutz und Datenschutzrecht können Probleme nicht nur aus einer zu schwach ausgestalteten Rechtsposition privater Akteure resultieren, sondern auch umgekehrt aus extensiven und verhältnismässig unflexiblen Berechtigungen. Die Möglichkeit etwa, eine bereits erteilte Einwilligung in die Verarbeitung eigener Daten nachträglich zu widerrufen,[10] mag einer aggregierten Datennutzung gleichsam den Boden unter den Füssen entziehen. Allerdings wäre hierbei auch zu fragen, ob die weitere Nutzung der aggregierten Daten und der auf ihnen beruhenden Ergebnisse bzw. Produkte bereits dann problematisch wird, wenn die Einwilligung zur Verarbeitung nur für einen sehr geringen Teil der Rohdaten entfällt. Der Verweis auf den Unterschied zwischen Personendaten und – sehr viel weitgehender nutzbaren – Sachdaten beseitigt jedenfalls die Schwierigkeiten schon deswegen nicht, weil mit den Möglichkeiten moderner Datenanalyse die Deanonymisierung vermeintlich neutraler Sachdaten zu Personendaten vielfach möglich ist.[11]

[Rz 9] Neuen und möglicherweise sehr weitreichenden Abstimmungsbedarf könnte die im Gesetzgebungsprozess befindliche Totalrevision des Datenschutzgesetzes mit sich bringen.[12] Als Beispiel genannt sei hier nur das durch Art. 23 E-DSG erweiterte Einsichtsrecht in Dokumente, welche unter Verwendung eigener Daten erstellt wurden. Ergäbe sich hieraus ein Recht, Transaktionsverträge über datenbasierte Unternehmensgeheimnisse einzusehen,[13] und würde dieses Recht auf breiter Front genutzt, so könnte die bisherige, vorwiegend bilaterale Struktur solcher

Transaktionen wohl nicht aufrechterhalten werden.

[Rz 10] Auch der Interaktion des Geheimnisschutzrechts mit anderen für die Datenwirtschaft relevanten Rechtsgebieten ist genügende Aufmerksamkeit zu schenken. Ohne dass dieser Gesichtspunkt hier entfaltet werden könnte, sei als Beispiel auf Urheberrechte an digitalen Werken, insbesondere Software, hingewiesen. Sowohl in Konstellationen, in denen ein derartiges Urheberrecht und ein auf dieselben Daten bezogenes Geheimnisschutzrecht in derselben Hand liegen, als auch dort, wo sich Urheber und Geheimnisherr unterscheiden, beide ihre Berechtigungen aber (unter anderem) aus derselben Datenquelle ableiten, können die urheberrechtlichen Nutzungs- und Verbotsrechte, aber auch die Urheberrechtsschranken und das aus ihnen folgende Nutzungsrecht der Allgemeinheit zu den Wertungen des Geheimnisschutzrechtes in Spannung geraten.

4. Geheimhaltung(sanreiz) – der Mechanismus der Zukunft?

[Rz 11] Der letzte Gesichtspunkt, den wir hier herausgreifen wollen, ist gegenüber den bereits genannten vielleicht noch fundamentaler. Er liegt in dem Bedenken, ob ein Regelsystem, das wie der Geheimnisschutz auf Abschottung und Vorenthaltung wertvoller Informationen basiert, den besten Mechanismus für die vordringende Datenwirtschaft anbietet. Denn das volle ökonomische und Wohlfahrtspotenzial eines verstärkt datenbasierten Wirtschaftens wird sich nur heben lassen, wenn ein weiter Kreis an Akteuren Datenzugang hat.[14] Auch politische, soziale und wettbewerbsrechtliche Gefahren durch konzentrierte Datenmacht in der Hand weniger grosser Marktteilnehmer werden nicht gemindert, wenn das Geheimnisschutzrecht in einer Ausgestaltung den zentralen Ordnungsrahmen bildet, die den beteiligten Akteuren Anreize für das möglichst intensive Anhäufen exklusiver Datenbestände setzt.

III. Gegenwärtige Regelungsinitiativen

[Rz 12] Die einschlägigen Regelungsvorhaben bzw. jüngst realisierten Regelungsprojekte in der Schweiz und der EU helfen bei den soeben angerissenen Problemstellungen wenig weiter. Die Strategie «Digitale Schweiz»[15] und die EU-Strategie für einen digitalen Binnenmarkt[16] nehmen auf den Geheimnisschutz überhaupt keinen konkreten Bezug. Anders ist dies naturgemäss bei der Know-how-Schutz-Richtlinie der EU;[17] diese bleibt jedoch weitestgehend in den bekannten Bahnen des Rechtsgebiets. Die Richtlinie lässt schon die Frage offen, ob und wann digitale Daten überhaupt Geschäftsgeheimnisse sein können. Das Verhältnis zu anderen Rechtsmaterien wird durch einen pauschalen Vorbehalt zugunsten der Anwendbarkeit sonstiger einschlägiger Regeln gelöst,[18] also gerade nicht durch ein durchdachtes Gesamtkonzept etwa für das Miteinander von Geheimnisschutz, Datenschutzrecht und Immaterialgüterrecht. Statt auf ein weiterentwickeltes Zuordnungskonzept setzt die Richtlinie ganz auf die klassischen, womöglich sogar restriktiver als bisher interpretierten,[19] Geheimhaltungsanforderungen als Schutzvoraussetzung. Eine grundlegende Neuorientierung des Geheimnisschutzes an den Bedürfnissen der Datenwirtschaft ist all dies nicht.

IV. Fazit und Ausblick

[Rz 13] In der Summe dürften vor allem zwei Handlungsalternativen mit unterschiedlichen Stossrichtungen in Betracht kommen, um den Geheimnisschutz auf die Bedürfnisse der Datenwirtschaft auszurichten. Entweder man schlägt gleichsam den Weg nach vorne ein und versucht, das Recht des Geheimnisschutzes zu einem umfassenden Ordnungsrahmen für die Datenwirtschaft um- und auszubauen. Die hierfür erforderlichen Modifikationen – nicht zuletzt an faktischer Informationskontrolle und erfolgreicher Geheimhaltung als zentralen herkömmlichen Zuordnungskriterien für die Berechtigung zur wirtschaftlichen Nutzung von Informationen – wären weitreichend. Man kann sich dann fragen, ob durch ihre Vornahme der Geheimnisschutz nicht zu einem sehr andersartigen, unter Umständen auch anders zu benennenden Rechtsgebiet würde. Zudem bleiben die fundamentalen Zweifel, ob das Geheimhalten der richtige Grundmechanismus für eine Datenwirtschaft ist, die eher auf Zugangsrechten basieren sollte. Dennoch: Von vorneherein ungangbar erscheint dieser Weg nicht, schon weil irgendeine ordnende und bei der marktmässigen Preisbildung helfende Zuordnungsregel das Gegengewicht zu weitreichenden

Zugangsrechten bilden muss, wie sie für die Datenwirtschaft unverzichtbar erscheinen. [20]

[Rz 14] Oder man setzt ein anderes Regelsystem als den Geheimnisschutz zum primären, mindestens aber mitprägenden Ordnungsrahmen der Datenwirtschaft. Das Geheimnisschutzrecht muss deswegen keineswegs massiv zurückgestutzt oder gar abgeschafft werden; dies wäre auch ein sehr drastischer Ansatz für ein fest etabliertes und ökonomisch bedeutsames Rechtsgebiet. Das Geheimnisschutzrecht kann vielmehr als partieller Lösungsansatz weiterbestehen, der für gewisse Konstellationen sachgerechten Schutz und eine sachgerechte Zuordnung ökonomischer Verwertungsmöglichkeiten anbietet. Möglicherweise wird seine Bedeutung dann vor allem in Bereichen liegen, die relativ weit von der Rohdatengewinnung entfernt sind und mit stark bearbeiteten Datenprodukten zu tun haben. Auch in einem solchen Modell bleiben freilich das Petitum nach einer sorgfältigen Abstimmung der involvierten Rechtsgebiete dringend und ein (begrenzter) Modifikationsbedarf am derzeitigen Geheimnisschutzrecht absehbar, damit nicht der Geheimnisschutz zum Bremsklotz und Störfaktor für die Datenwirtschaft werde.

Prof. Dr. Peter Georg Picht, LL.M. (Yale), Professor für Handels- und Wirtschaftsrecht an der Universität Zürich; Affiliated Research Fellow Max Planck Institute for Innovation and Competition, Munich; Geschäftsleitung CIPCO – Center for Intellectual Property and Competition Law, Universität Zürich.

---

1 Als weitere Bestimmungen liessen sich nennen Art. 273 StGB (wirtschaftlicher Nachrichtendienst), Art. 47 Bankengesetz (BankG) (Verletzung des Berufsgeheimnisses), Art. 3 lit. b Bundesgesetz über den Datenschutz (DSG) (Datenschutz für juristische Personen), Art. 156 Zivilprozessordnung (ZPO) (Vertrauensschutz im Zivilprozess).

2 Ramon Mabillard, in: Peter Jung/Philippe Spitz (Hrsg.), Bundesgesetz über den unlauteren Wettbewerb (UWG) – Stämpflis Handkommentar, Stämpfli, 2. Auflage, Bern 2017, Art. 6 N 8 ff.

3 Alois Troller, Immaterialgüterrecht 1 – Patentrecht, Markenrecht, Urheberrecht, Muster- und Modellrecht, Wettbewerbsrecht, Helbing & Lichtenhahn, Basel 1983, 421; Mario M. Pedrazzini/Federico A. Pedrazzini, Unlauterer Wettbewerb UWG, Stämpfli, 2. Auflage, Bern 2002, N 8.44; Markus R. Frick, in: Reto M. Hilty/Reto Arpagaus (Hrsg.), Bundesgesetz über den unlauteren Wettbewerb (UWG) – Basler Kommentar, Helbing & Lichtenhahn, Basel 2013, Art. 6 N 19.

4 Rolf H. Weber/Florent Thouvenin/Alfred Früh, Data Ownership: Taking Stock and Mapping the Issues, in: Matthias Dehmer/Frank Emmert-Streib (eds.), Frontiers in Data Science, CRC Press, Boca Raton 2017, 111, 131 f.

5 Florent Thouvenin/Alfred Früh/Alexandre Lombard, Eigentum an Sachdaten: Eine Standortbestimmung, SZW 2017, 25 ff., 30; eingehend Herbert Zech, Information als Schutzgegenstand, Mohr Siebeck, Tübingen 2012, 230 ff., mit Darstellung der verschiedenen Sichtweisen.

6 Troller (Fn. 3), 417; Carl Baudenbacher/Jochen Glöckner, in: Carl Baudenbacher (Hrsg.), Lauterkeitsrecht – Kommentar zum Gesetz gegen den unlauteren Wettbewerb (UWG), Helbing & Lichtenhahn, Basel 2001, Art. 6 N 44.

7 S. eingehend hierzu die, unter anderem gemeinsam mit dem Fraunhofer Institut, erarbeitete Studie des BMVI, «Eigentumsordnung» für Mobilitätsdaten?, http://www.bmvi.de/SharedDocs/DE/Artikel/DG/studie-mobilitaetsdaten-fachkonsultation.html (alle Websites zuletzt besucht am 4. Dezember 2017).

8 BMVI (Fn. 7), 61 f.

9 Für unterschiedliche Ausprägungen dieses Ansatzes s. Herbert Zech, Daten als Wirtschaftsgut – Überlegungen zu einem «Recht des Datenerzeugers», CR 2015, 137, 144 ff.; Louisa Specht, Ausschließlichkeitsrechte an Daten – Notwendigkeit, Schutzumfang, Alternativen, CR 2016, 288, 295; BMVI (Fn. 7), 105.

10 Bruno Baeriswyl, in: Bruno Baeriswyl/Kurt Pärli, Dateschutzgesetz (DSG) – Stämpflis Handkommentar, Stämpfli, Bern 2015, Art. 4 Rn. 57 mwN.

11 S. hierzu etwa Clara-Ann Gordon, Daten aus Selbstvermessung, digma 2016, 70, 73 f.; Rolf H. Weber/Dominic Oertly, Aushöhlung des Datenschutzes durch De-Anonymisierung bei Big Data Analytics?, in: Jusletter IT 21. Mai 2015.

12 Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz, BBl 2017 6941.

13 Eingehend David Rosenthal, Der Entwurf für ein neues Datenschutzgesetz, in: Jusletter 27. November 2017, Rz. 106 ff.

14 Vgl. auch Ausschließlichkeits- und Zugangsrechte an Daten – Positionspapier des Max-Planck-Instituts für Innovation und Wettbewerb vom 16. August 2016 zur aktuellen europäischen Debatte, http://www.ip.mpg.de/de/link/positionspapier-2016-08-16.html, 2 f.

15 Vgl. https://www.bakom.admin.ch/infosociety.

16 Vgl. http://europa.eu/rapid/press-release_IP-15-4919_de.htm; Mitteilung der Kommission an das europäische Parlament, den Rat, den europäischen Wirtschafts- und Sozialausschusss und den Ausschuss der Regionen: Strategie für einen digitalen Binnenmarkt für Europa, 6. Mai 2015, COM(2015) 192 final.

17 Richtlinie (EU) 2016/943 des Europäischen Parlaments und des Rates vom 8. Juni 2016 über den Schutz vertraulichen

Know-hows und vertraulicher Geschäftsinformationen (Geschäftsgeheimnisse) vor rechtswidrigem Erwerb sowie rechtswidriger Nutzung und Offenlegung, ABl. L 157/1 vom 15. Juni 2016.

18 Vgl. Erwägungsgründe (37)–(39), Art. 1 Abs. 2 Richtlinie (EU) 2016/943.

19 S.a. Stellungnahme des Max-Planck-Instituts für Innovation und Wettbewerb vom 3. Juni 2014, http://www.ip.mpg.de/fileadmin/ipmpg/content/stellungnahmen/stellungnahme-geschaeftsgeheimnisse_2014-05-12_final_7.pdf, 6.

20 Vgl. auch Positionspapier des Max-Planck-Instituts für Innovation und Wettbewerb (Fn. 14).